UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/666,341	09/22/2003	Jun Takeda	04329.3143	8385

22852 7590 03/12/2009	EXAMINER	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP	ARCHER, CHRISTOPHER B	
901 NEW YORK AVENUE, NW	ART UNIT	PAPER NUMBER
WASHINGTON, DC 20001-4413	2432	

MAIL DATE	DELIVERY MODE
03/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/666,341	TAKEDA, JUN
	Examiner	Art Unit	
	CHRISTOPHER B. ARCHER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _18 April 2005_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-16_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _22 September 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _See Continuation Sheet_.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :09/22/2003;01/13/2005;04/18/2005.

DETAILED ACTION

1.   The instant application having Application No. 10/666,341 filed on 09/22/2003 is presented for examination by the examiner.

Oath/Declaration

2.   The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63**.

Priority

3.   As required by **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on 10/10/2002 (Japan 2002-297550).

        Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

4.   The disclosure is objected to because of the following informalities:

        Page 6, lines 13-14:

        The phrase "identify a RADIUS server which is to authenticate that server" is indefinite. The second use of the word server is confusing.

        Page 11, lines 1 and 9:

The stations 40(A) and 40(B) are referred to by the abbreviation "ATA." This abbreviation is found nowhere else in the specification. For the purpose of examination, the examiner treated these as equivalent to "STA" as is used to refer to other stations.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6.   The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

Regarding claim 2:

There is insufficient antecedent basis for the limitation "each domain."

The phrase "the server exists for each domain" is unclear. It is unknown whether multiple servers exist, one server for each domain, or one server exists for all of the domains.

The phrase "the terminal exists without being set to the domains" is unclear. For the purposes of examination, the examiner considers this to mean that the terminal is portable and can therefore attempt to connect to any remote domain.

Regarding claim 3:

The phrase "when the requesting terminal belongs to the domain to which it belongs" is indefinite.

Regarding claim 15:

The steps involved in the method of claim 15 are unclear. For the purposes of examination, the examiner assumes that three steps are involved:

1. Receiving authentication request from the terminal;

2. Identifying an authentication server for that terminal; and

3. Connecting the requesting terminal to the correct authentication server.

Claim Rejections - 35 USC § 102

7.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8.   Claims 7 and 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Crane et al. (US 6,510,236), hereafter referred to as Crane.

Regarding claim 7:

Crane discloses "A repeater for use in a network system having servers each of which authenticates a terminal upon receipt of an access request therefrom, comprising:

an identifying unit configured to identify a server which is to authenticate a requesting terminal, upon reception of a request for authentication from the terminal; and

a connecting unit configured to connect the requesting terminal to the identified server."

[(Crane column 2, lines 29-38 and Crane column 4, line 48 to column 5, line 36) discloses a system that passes client information to an application server. The application server then locates an authentication server and redirects the authentication data to the authentication server. The authentication server verifies that the authentication data is acceptable for authentication.]

Regarding claim 11:

Crane discloses "A network system comprising:

one supplicant which needs authentication when making access to a network;

authentication server which perform authentication; and

an authenticator which, in response to receipt of a request for authentication from a supplicant, identifies an authentication server which is to authenticate the requesting supplicant and connects the requesting supplicant to the identified authentication server."

[(Crane column 2, lines 29-38 and Crane column 4, line 48 to column 5, line 36) discloses a system that passes client information to an application server. The application server then locates an authentication server and redirects the authentication data to the authentication server. The authentication server verifies that the authentication data is acceptable for authentication.]

Claim Rejections - 35 USC § 103

9.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

10.   Claims 1-6, 8, 12, 15, and 16 are rejected under 35 U.S.C. 102(e) as being unpatentable

over Crane, in view of Liu et al. (US 5,898,780), hereafter referred to as Liu.

Regarding claim 1:

Crane discloses "A network system comprising:

a terminal which makes access to a network;

a server which, when an access request is made by a terminal, authenticates the

requesting terminal; and

a processing device which receives an authentication request from a terminal,

identifies a server which authenticates the terminal," and "connects the requesting

terminal to the identified server," but fails to explicitly disclose "based on information

received from the terminal at the time of reception of the request."

[(Crane column 2, lines 29-38 and Crane column 4, line 48 to column 5, line

36) discloses a system that passes client information to an application server. The

application server then locates an authentication server and redirects the

authentication data to the authentication server. The authentication server verifies

that the authentication data is acceptable for authentication.]

However, Liu discloses "based on information received from the terminal at the time of reception of the request."

[(Liu column 5, lines 5-40) discloses a system that uses login information to locate a correct authentication server.]

Crane and Liu are analogous art because they are from the same field of endeavor of remote device and user authentication.

It would have been obvious to one of ordinary skill in the art at the time of invention to use login information from the terminal to locate the correct authentication server, as described in Liu, in order to hasten the verification process and prevent possible redundant or erroneous authentication server identification attempts.

Regarding claim 2:

Crane discloses "The network system according to claim 1," but fails to explicitly disclose "wherein the server exists for each domain and the terminal exists without being set to the domains."

However, Crane combined with Liu discloses "wherein the server exists for each domain and the terminal exists without being set to the domains."

[(Crane column 4, line 48 to column 5, line 36) discloses a system in which each device type has its own authentication server. These device types may include token card readers. In this manner, the token card is not bound to a single computer or location.

(Liu column 4, lines 50-61) discloses a system that uses an entry log table to locate an authentication server within a remote domain.]

Regarding claim 3:

Crane discloses "The network system according to claim 1," and "the process of connecting the requesting terminal to the identified server," but fails to explicitly disclose "wherein the processing device, upon receipt of the request from the terminal, identifies a domain to which the requesting terminal belongs and, when the requesting terminal belongs to the domain to which it belongs, performs the process of identifying a server."

However, Liu discloses "wherein the processing device, upon receipt of the request from the terminal, identifies a domain to which the requesting terminal belongs and, when the requesting terminal belongs to the domain to which it belongs, performs the process of identifying a server."

[(Liu column 4, lines 50-61) discloses a system that uses an entry log table to locate an authentication server within a remote domain.]

Regarding claim 4:

Crane further discloses "wherein the processing device and the terminal are connected via a wireless LAN."

[(Crane column 1, lines 25-26) shows that wireless or wireline connections are both acceptable methods of connecting from a computer to a server.]

Regarding claim 5:

Crane discloses "An information processing device comprising:

a receiving unit configured to receive a request for authentication from a terminal which makes access to a network;

an identifying unit configured to identify a device which verifies the eligibility of the requesting terminal to make access to the network;" and

"a connecting unit configured to connect the requesting terminal to the identified device" but fails to explicitly disclose "based on the received authentication request."

[(Crane column 2, lines 29-38 and Crane column 4, line 48 to column 5, line 36) discloses a system that passes client information to an application server. The application server then locates an authentication server and redirects the authentication data to the authentication server. The authentication server verifies that the authentication data is acceptable for authentication.]

However, Liu discloses "based on the received authentication request."

[(Liu column 5, lines 5-40) discloses a system that uses login information to locate a correct authentication server.]

Crane and Liu are analogous art because they are from the same field of endeavor of remote device and user authentication.

It would have been obvious to one of ordinary skill in the art at the time of invention to use login information from the terminal to locate the correct authentication server, as described in Liu, in order to hasten the verification process and prevent possible redundant or erroneous authentication server identification attempts.

Regarding claim 6:

Crane discloses "The information processing device according to claim 5," but fails to explicitly disclose "wherein the identifying unit obtains the identification name of the requesting terminal from information received from the terminal when the authentication request is received, recognizes a domain to which the requesting terminal belongs through a matching operation on the identification name, and identifies the device which verifies the eligibility of the requesting terminal to make access to the network based on the result of the recognition."

However, Liu discloses "wherein the identifying unit obtains the identification name of the requesting terminal from information received from the terminal when the authentication request is received, recognizes a domain to which the requesting terminal belongs through a matching operation on the identification name, and identifies the device which verifies the eligibility of the requesting terminal to make access to the network based on the result of the recognition."

[(Liu column 4, lines 50-61) discloses a system that uses an entry log table to locate an authentication server within a remote domain.]

Regarding claim 8:

Crane discloses "The repeater according to claim 7," but fails to explicitly disclose "wherein the identifying unit has a table which manages a plurality of network connectable domains and servers each of which is placed in one of the domains in a

mapped form and identifies a server which is to authenticate the requesting terminal based on information from the terminal at the time of reception of the request and the table."

However, Liu discloses "wherein the identifying unit has a table which manages a plurality of network connectable domains and servers each of which is placed in one of the domains in a mapped form and identifies a server which is to authenticate the requesting terminal based on information from the terminal at the time of reception of the request and the table."

[(Liu column 4, lines 50-61) discloses a system that uses an entry log table to locate an authentication server within a remote domain.]

Crane and Liu are analogous art because they are from the same field of endeavor of remote device and user authentication.

It would have been obvious to one of ordinary skill in the art at the time of invention to locate the authentication server using a domain name, as disclosed in Liu, as this allows for quicker location of a remote terminal's home authentication server.

Regarding claim 12:

Crane discloses "The network system according to claim 11," but fails to explicitly disclose "wherein the authenticator has a table which manages a plurality of network connectable domains and authentication servers each of which is placed in one of the domains and identifies a server which is to authenticate the requesting terminal by obtaining identification information of the requesting terminal at the time of reception of

the request and performing pattern matching between the domain set in the table and the identification information."

However, Liu discloses "wherein the authenticator has a table which manages a plurality of network connectable domains and authentication servers each of which is placed in one of the domains and identifies a server which is to authenticate the requesting terminal by obtaining identification information of the requesting terminal at the time of reception of the request and performing pattern matching between the domain set in the table and the identification information."

[(Liu column 4, lines 50-61) discloses a system that uses an entry log table to locate an authentication server within a remote domain.]

Crane and Liu are analogous art because they are from the same field of endeavor of remote device and user authentication.

It would have been obvious to one of ordinary skill in the art at the time of invention to locate the authentication server using a domain name, as disclosed in Liu, as this allows for quicker location of a remote terminal's home authentication server.

Regarding claim 15:

Crane discloses "A method of building a network system having a terminal each of which make access to a network, a repeater which allows a terminal to make access to the network according to an access request from it, and one server, when an access request is made by a terminal, authenticates the requesting terminal,

the allowing the terminal to make access includes receiving an authentication request from a terminal, identifying a server which is to authenticate that terminal," and "connecting the requesting terminal to the identified server," but fails to explicitly disclose "based on information received from the terminal"

[(Crane column 2, lines 29-38 and Crane column 4, line 48 to column 5, line 36) discloses a system that passes client information to an application server. The application server then locates an authentication server and redirects the authentication data to the authentication server. The authentication server verifies that the authentication data is acceptable for authentication.]

However, Liu discloses "based on information received from the terminal."

[(Liu column 5, lines 5-40) discloses a system that uses login information to locate a correct authentication server.]

Crane and Liu are analogous art because they are from the same field of endeavor of remote device and user authentication.

It would have been obvious to one of ordinary skill in the art at the time of invention to use login information from the terminal to locate the correct authentication server, as described in Liu, in order to hasten the verification process and prevent possible redundant or erroneous authentication server identification attempts.

Regarding claim 16:

Crane discloses "The method according to claim 15," but fails to explicitly disclose "wherein the identifying the server identifies a server which is to authenticate the

requesting terminal based on a table which manages a plurality of network connectable

domains and servers each of which is placed in a respective one of the domains in a

mapped form and identification information obtained from the terminal at the time of

receipt of the request."

However, Liu discloses "wherein the identifying the server identifies a server

which is to authenticate the requesting terminal based on a table which manages a

plurality of network connectable domains and servers each of which is placed in a

respective one of the domains in a mapped form and identification information obtained

from the terminal at the time of receipt of the request."

[(Liu column 4, lines 50-61) discloses a system that uses an entry log table to

locate an authentication server within a remote domain.]

11.   Claims 9, 10, 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Crane in view of McIntosh et al. (US 2003/0139180), hereafter referred to as McIntosh.

Regarding claim 9:

Crane discloses "The repeater according to claim 7," but fails to explicitly

disclose "wherein the repeater performs the authentication procedure with the requesting

terminal according to the definitions specified in the IEEE 802.1x."

However, McIntosh discloses "wherein the repeater performs the authentication

procedure with the requesting terminal according to the definitions specified in the IEEE

802.1x."

[(McIntosh [0089]) shows an authentication system that uses IEEE 802.1x.]

Crane and McIntosh are analogous art because they are from the same field of endeavor of secure remote access.

It would have been obvious to one of ordinary skill in the art at the time of invention to use IEEE 802.1x, as disclosed in McIntosh, in the authentication scheme of Crane, as IEEE 802.1x is a widely know WLAN standard.

Regarding claim 10:

Crane discloses "The repeater according to claim 7," but fails to explicitly disclose "wherein the repeater performs the authentication procedure with the requesting terminal according to the EAP authentication protocol."

However, McIntosh discloses "wherein the repeater performs the authentication procedure with the requesting terminal according to the EAP authentication protocol."

[(McIntosh [0089]) shows an authentication system that uses Extensible Authentication Protocol as its authentication framework.]

Crane and McIntosh are analogous art because they are from the same field of endeavor of secure remote access.

It would have been obvious to one of ordinary skill in the art at the time of invention to utilize Extensible Authentication Protocol, as disclosed in McIntosh, in the authentication scheme of Crane, as EAP allows the WLAN access points to support a wide range of authentication methods.

Regarding claim 13:

Crane discloses "The network system according to claim 11," but fails to explicitly disclose "wherein the authenticator performs the authentication procedure with the requesting supplicant according to the definitions specified in the IEEE 802.1x."

However, McIntosh discloses "wherein the authenticator performs the authentication procedure with the requesting supplicant according to the definitions specified in the IEEE 802.1x."

[(McIntosh [0089]) shows an authentication system that uses IEEE 802.1x.]

Crane and McIntosh are analogous art because they are from the same field of endeavor of secure remote access.

It would have been obvious to one of ordinary skill in the art at the time of invention to use IEEE 802.1x, as disclosed in McIntosh, in the authentication scheme of Crane, as IEEE 802.1x is a widely know WLAN standard.

Regarding claim 14:

Crane discloses "The network system according to claim 11," but fails to explicitly disclose "wherein the authenticator performs the authentication procedure with the requesting supplicant according to the EAP authentication protocol."

However, McIntosh discloses "wherein the authenticator performs the authentication procedure with the requesting supplicant according to the EAP authentication protocol."

[(McIntosh [0089]) shows an authentication system that uses Extensible Authentication Protocol as its authentication framework.]

Crane and McIntosh are analogous art because they are from the same field of
endeavor of secure remote access.

It would have been obvious to one of ordinary skill in the art at the time of
invention to utilize Extensible Authentication Protocol, as disclosed in McIntosh, in the
authentication scheme of Crane, as EAP allows the WLAN access points to support a
wide range of authentication methods.

Conclusion

12.   The prior art made of record and not relied upon is considered pertinent to applicant's
disclosure.

Farber et al. (US 6,185,598) – discusses repeaters for locating user requested
resources.

Roskind et al. (US 2003/0163730) – discloses a distributed authentication system
with multiple users and multiple authentication servers.

White (US 6,826,692) – discloses a distributed authentication system with
multiple users and multiple authentication servers.

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to CHRISTOPHER B. ARCHER whose telephone number is (571)
270-7308. The examiner can normally be reached on M-F 7:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. B. A./
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432